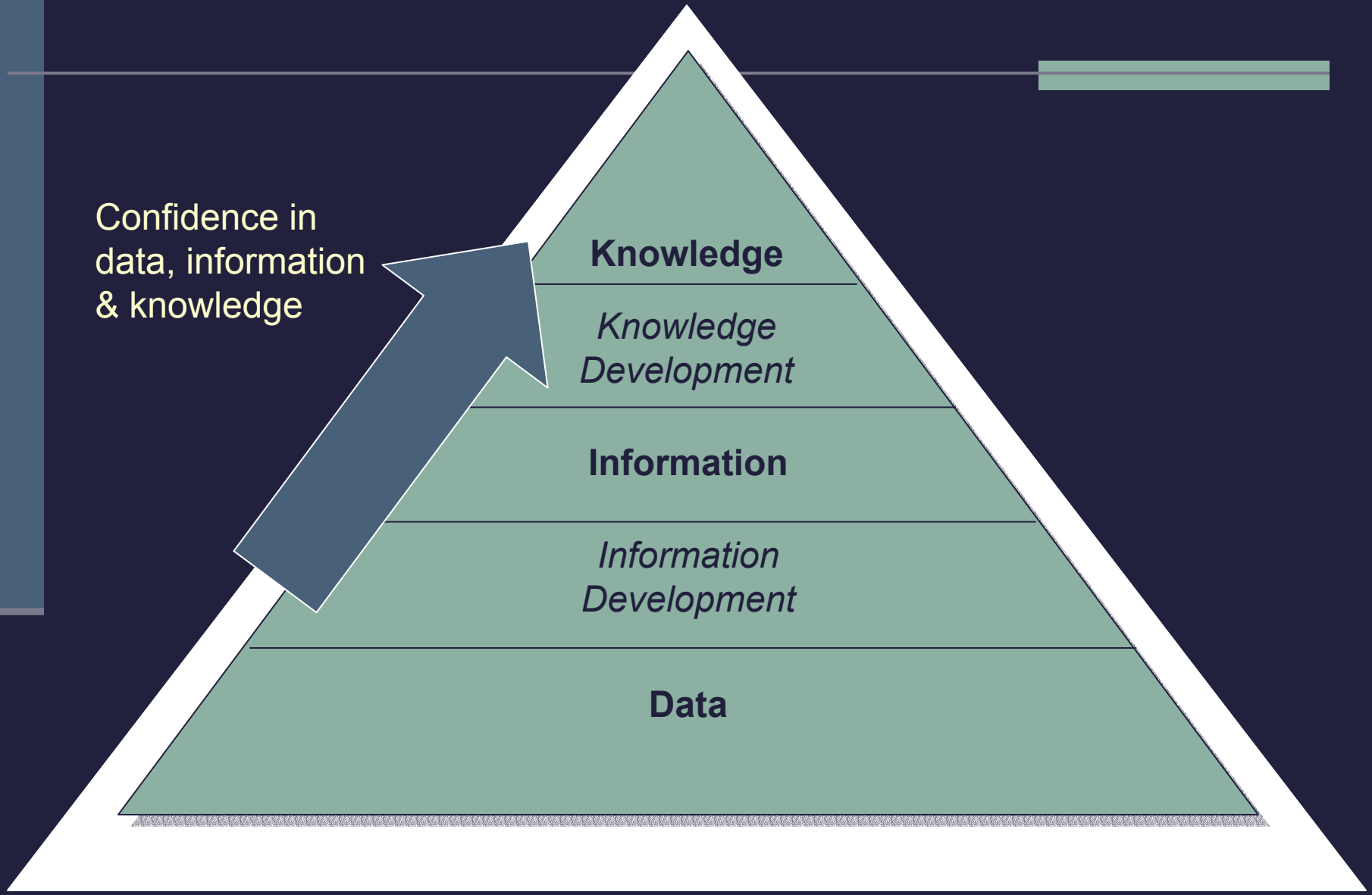
Trustworthy Computing

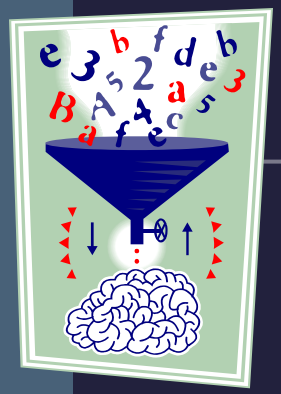
Lisa Carnahan
Computer Scientist
NIST/Information Technology Laboratory
lisa.carnahan@nist.gov

June 10, 2003

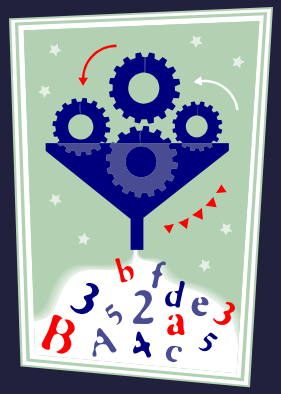
Information and Knowledge Management



Motivation



- Good decisions require a confidence in the information used
- Our customers recognize need for a confidence in IT systems that produce the information



Is the IT system doing what I expect?

Are my measurements provably correct?

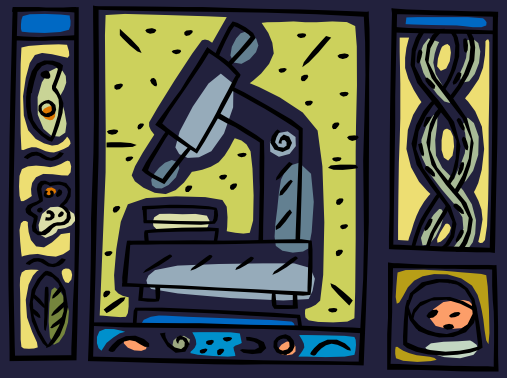
Has the data been tampered with?

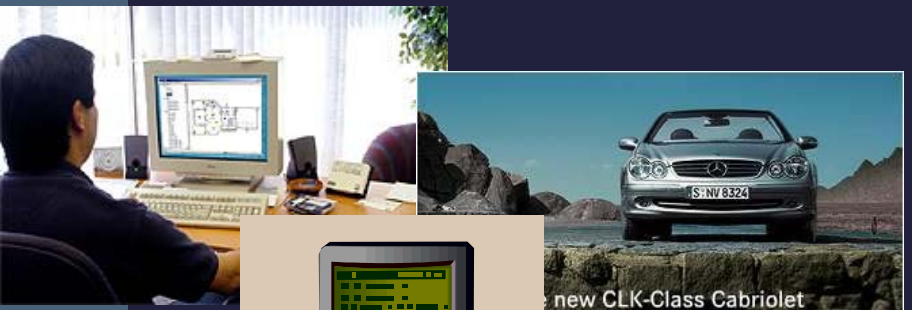
Am I acquiring the relevant data?

Will data be available when I need it?

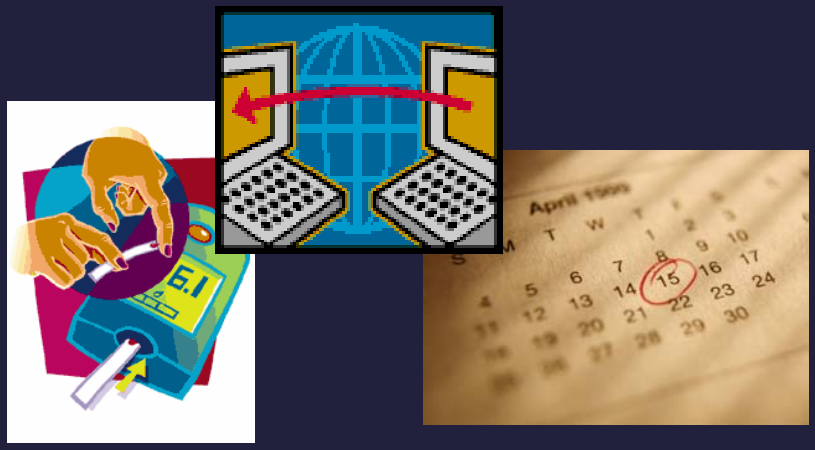
Trust & confidence in IT systems are a growing national need

Basis of science moving forward





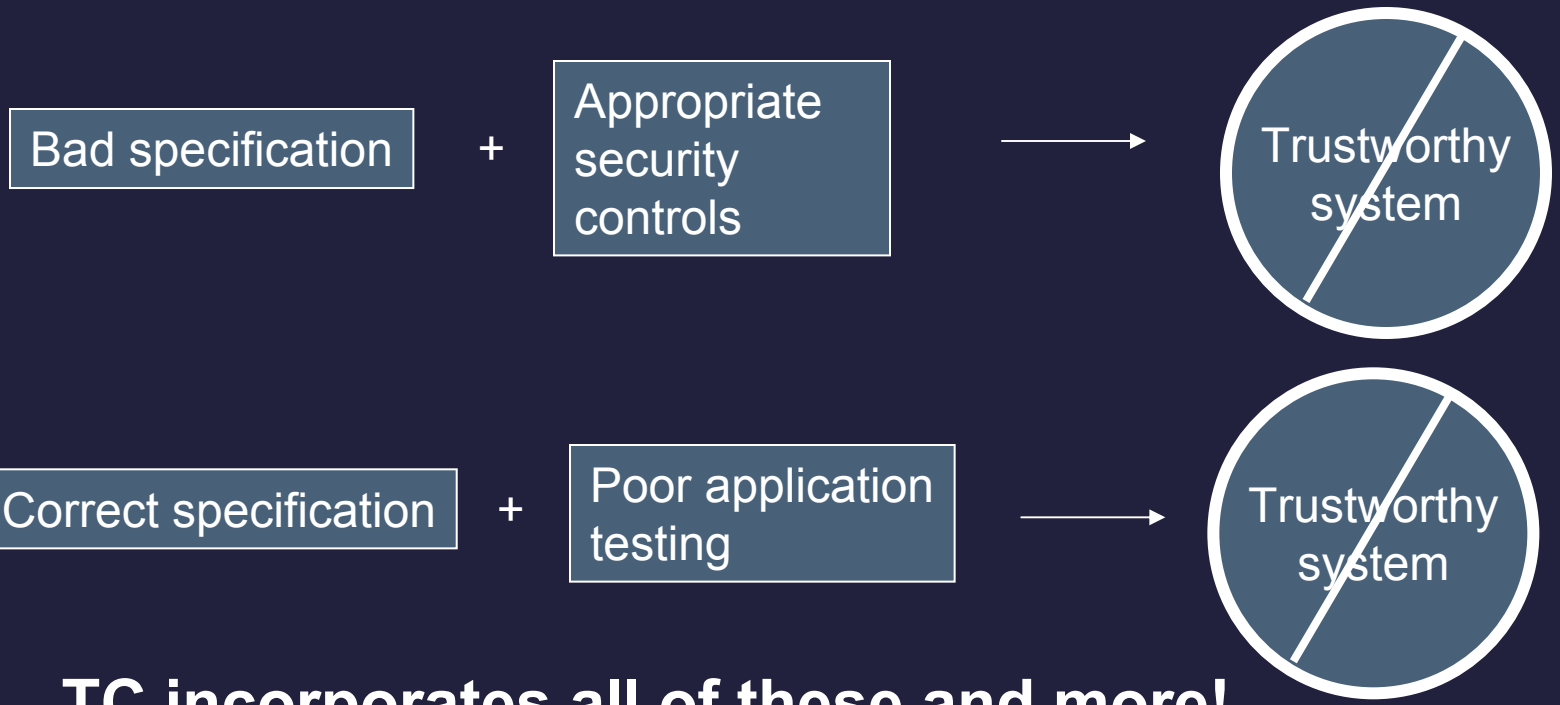
Expanding use in our lives



Personal Situations

Trustworthy Computing is not …

- Not just security
- Not just software engineering
- Not just Conformance testing
- Not just system testing



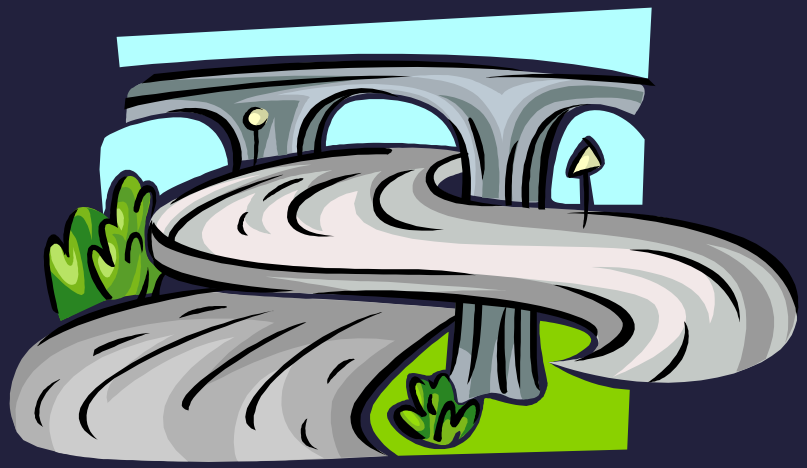
TC incorporates all of these and more!

Trustworthy Computing

- TC is the vehicle for achieving a level of reliability that results in complete confidence in the system output.
- Systemic approach
- Addressing multiple aspects
  - Functionality
  - Performance
  - Security
  - Dependability
  - …

Why aren't systems trustworthy?

- Degree varies by industry
- Not a focus throughout life of system
- Lack of standards
- No basis for measurement & testing



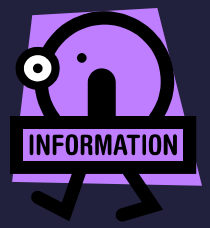
A Path Forward

- Industry paradigm shift
  - Industry recognizes the value
  - Industry must invest resources
- ITL provides
  - Standards
  - Measurements
  - Methods
  - Technology transfer

Responding to Our Customers

- Requirements are customer-driven
- Solutions based on standards & measurements

- Infrastructure technologies should be functionally correct
  - Network protocol testing
  - XML technology testing
- Dynamically combined systems should be robust and secure.



Enabling technologies must contribute to the confidence in a system

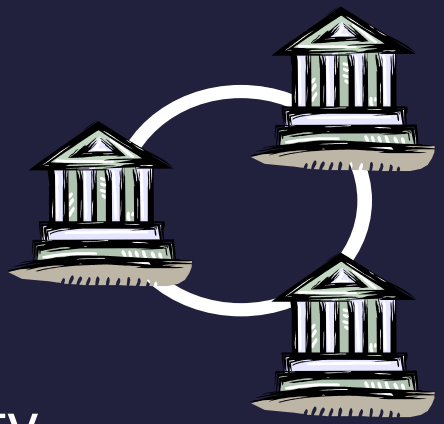
- Exploration of standards & measurement requirements in voting systems
  - Human factors
  - System integration
  - Electronic voting security

Our citizens demand trust in their voting systems and election processes

Voting Systems	Financial Community	Healthcare Community	Homeland Security
Enabling Technologies			

- Traditionally focused on trust
- Certifications based on NIST security and cryptographic standards & tests
  - BITS
  - Visa International
  - Smart Card Security User Group

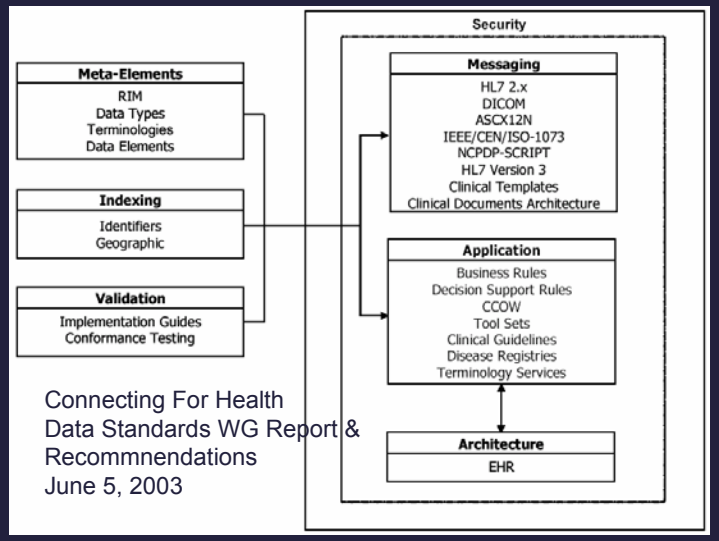
The level of trust in our financial institutions must remain high as services become automated.



NIST National Institute of Standards and Technology

- Healthcare informatics
  - Conformance test development for information exchange
    - HL7
    - IEEE 1073
  - Markle Foundation's Connecting for Health
- Future Needs for Standards Workshop-Nov '03

Patients must not suffer harm from errors and inadequacies in our healthcare information, diagnostic and care systems.



Connecting For Health
Data Standards WG Report & Recommnendations
June 5, 2003

Voting Systems	Financial Community	Healthcare Community	Homeland Security
Enabling Technologies			

- Computer Forensics
  - Confidence in tools used by investigators
  - Robust testing results meet legal scrutiny- Daubert requirements for scientific evidence
- Biometrics
  - Confidence in the identity of people entering our borders
  - Performance testing based on metrics

Homeland Security requires trust in the IT tools used to protect the homeland.

A New Challenge: Data Preservation

- Technology allows us to electronically store vast amounts of information
- Can today's info be accessible far in the future?
  - Media longevity
  - Tools to access

- Preliminary success in media measurements
- Exploring areas to broaden scope

Summary

- Trustworthy computing enables confidence in computed data & information
- Standards & measurements are key to achieving trustworthy computing
- ITL is taking a systemic approach
- Data preservation is a new challenge

Why aren't systems trustworthy?

- Degree varies by industry
- [illegible] of
- [illegible] rds
- No basis for measurement & testing

A Path Forward

- Industry paradigm shift
  - Industry recognizes the [illegible]
  - [illegible] est
- [illegible]
  - Standards
  - Measurements
  - Methods
  - Technology transfer